



Symantec™ Endpoint Protection 14.3 RU9 Release Notes

Updated: June 2024



Table of Contents

What's new for Symantec Endpoint Protection 14.3 RU9?..... 3

System requirements for Symantec Endpoint Protection (SEP) 14.3 RU9..... 8

Known issues and workarounds for Symantec Endpoint Protection (SEP)..... 17

**Supported and unsupported upgrade paths to the latest version of Symantec
Endpoint Protection..... 29**

Where to get more information..... 31

What's new for Symantec Endpoint Protection 14.3 RU9?

These sections describe the new features in this release.

Symantec Endpoint Protection Manager

- The **Enable Browser Intrusion Prevention for Windows** option in the Intrusion Prevention policy automatically loads the Google Chrome and Microsoft Edge browser extensions for Symantec Endpoint Protection. However, this option overrides third-party extensions that organizations install if they use a different management tool. 14.3 RU9 provides an option that allows you to install and manage the extension with your tool of choice, such as Chrome Browser Cloud Management or Microsoft InTune.

To access this option, go to an Intrusion Prevention policy and make sure that the **Enable Browser Intrusion Prevention for Windows** option is selected and that the **Enable third-party management of extensions** option is cleared.

See: [Integrating browser extensions with Symantec Endpoint Protection \(SEP\) to protect against malicious websites](#)

- Fixed the following issues when Symantec Endpoint Protection Manager uses public CA-signed certificates as a result of adding Transport Layer Security (TLS) host name validation in 14.3 RU8:

- The Symantec Endpoint Protection Manager installation and upgrade requires that the management server name must also match one or more of the Subject Alternate Names (SANs) that are listed in the server certificate. In addition, the server name must use a valid host name, fully qualified domain name (FQDN), or IP address. If the server name and the SAN do not match, you must rename the server before you can continue.

See: [Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate \(14.3 RU9 or later\)](#)

- If Symantec Endpoint Protection Manager detects that the replication partner host name or IP address does not match one or more of the SANs for Symantec Endpoint Protection Manager, Symantec Endpoint Protection Manager allows the upgrade. After the upgrade, you can reenable verification for increased security.

To access this option, right-click the replication partner site, click **Edit Replication Partner Properties**, and clear the **Disable verification of the partner server hostname** option.

To fix this issue, see: [Symantec Endpoint Protection Manager detected that the configured replication partner requires certificate verification to be disabled \(14.3 RU9 or later\)](#)

- When you log on to the Symantec Endpoint Protection Manager, you may see the following message about server certificates:

The server certificate could not be validated.

This message was in earlier releases, but provides additional information about why you see this error, including: You changed the computer hostname or IP address, or updated the server certificate recently. You need to use a valid hostname or IP address that matches your server certificate to log on to the Symantec Endpoint Protection Manager.

To fix this issue, see: [Error: Your server certificate is not valid because the computer host name or IP address changed \(14.3 RU8 or later\)](#)

- In earlier releases, to block the Symantec Endpoint Protection Manager from uploading file submissions, you had to configure your firewall to block the file submission URLs. 14.3 RU9 lets you allow or block file submissions through the **Suspicious files pseudonymously to Symantec to enhance threat protection intelligence** option, which is allowed by default.

To access this option, go to **Clients > Policies tab > External Communications > Submissions tab > More options**.

- Improved the following hybrid management issues:

- In large organizations with multi-site replication between Symantec Endpoint Protection Manager and the cloud server, the synchronization may not occur correctly. The cloud sometimes underreports the number of groups

or clients. In 14.3 RU9, before you migrate groups from the Symantec Endpoint Protection Manager using the **Switch Group to Cloud Managed** command, you can resynchronize the group hierarchy by running the

```
ASSET_SYNC_RESET
```

command. You can use this command to resynchronize up to 5,000 clients.

To view the event after you run the command, go to **Monitors > Log tab > System log type > Server Activity** content type. The following message appears:

The Symantec Endpoint Protection Bridge Service asset collector was reset successfully. All

- Symantec Endpoint Protection Manager now displays the following event when cloud unenrollment is successful but the API call to the cloud server fails:

Cloud unenrollment was successful on Symantec Endpoint Protection Manager but unsuccessful on the cloud server. Go to the **Integration** page to remove all the data.

To access these log events, go to **Monitors > Log tab > System log type > Server Activity** content type.

To unroll the management server from the cloud console, see: [Enrolling and unenrolling Symantec Endpoint Protection Manager domains from the cloud server](#)

- The cloud connector uploads data successfully after the proxy configuration changes.
- Reduced unnecessary traffic to the cloud server on the operational state of the client.
- Improved data collection for environments with multi-site replication.
- Improved consistency of data between the Symantec Endpoint Protection Manager and the cloud console.
- Clarified the description of how the management server sends data if it is enrolled in the cloud console.

Go to the **Admin** page > **Servers > Site Properties** page > **General** tab. The following figure displays the description that you see above the **Move Up** and **Move Down** buttons.

Site Properties for Local Site (Site [redacted])

General LiveUpdate Passwords Data Collection Private Insight Server

Site Settings

Site Name: Site [redacted]

Description: [redacted]

Console Timeout: 1 hour

☐ Keep track of every application that the clients run

☐ Delete learned application data after: 30 days

The management console uses the first management server in the list to send reports and notifications. If the management server is enrolled in the cloud, it sends data to the cloud server. If a server is not available, the console uses the next server in the list. You can change the priority of servers by using the Move Up and Move Down buttons.

[redacted] Move Up Move Down

See: [Site Properties: General](#)

- Reporting includes the following enhancements:
 - You can configure secure communication (TLS) to the Syslog server.
 You can access this option on the **External Logging** dialog box > **General** tab. In the **Destination Port** drop-down list, select **TLS**.

External Logging for Local Site (Site [redacted])

General Log Filter

Send logs to a Syslog Server or export to a file.

Update Frequency: 30 seconds Primary Logging Server: [redacted]

☒ Enable Transmission of Logs to a Syslog Server

Syslog Server: [redacted]

Destination Port: TLS 6666

Log Facility: UDP

Log Line Separator: TLS

See: [Exporting data to a Syslog server](#)

- The Syslog report includes a **Correlation ID** field for the TAA incident ID.
- The newly added **14.3 RU5 and later** Client Install Feature Set no longer requires SONAR Protection (Behavioral Analysis) to be installed when Advanced Download Protection is installed.
To view this option, go to the **Admin** page > **Install Packages** > **Add Client Install Feature Set**, and then click the **Feature set version** drop-down list.

Add Client Install Feature Set

Name: [redacted]

Description: [redacted]

Feature sets for all previous versions are created automatically. You can also manually edit feature sets for previous versions.

Feature set version: 14.3 RU5 and later

☒ Virus, Spyware, and Basic Download Protection
☒ Advanced Download Protection
☐ Microsoft Outlook Scanner

☒ Proactive Threat Protection
☒ SONAR Protection
☒ Application and Device Control

Feature Description:
Installs components for zero-day detection of viruses and spywares.

Required component(s):

See: [Choosing which security features to install on the client](#)

- The REST API supports the following commands:
 - To quickly add a large number of IP addresses and MAC addresses into a firewall rule, you can import a list of existing addresses into a host group, and then use a set of REST APIs that supports the GET, POST, and PUT methods for host groups.
See: [Symantec Endpoint Protection API commands](#)
 - For compliance reporting, you can find update details for the IPS and Behavioral Analysis by using these REST API commands: GET /api/v1/computers returns ipsDefsetVersion and GET /api/v1/computers returns behavioralAnalysisDefsetVersion.
- The following third-party components were upgraded or added:

- Apache Commons Codec
- Apache Commons Compress
- Apache Commons IO
- Apache Commons Lang
- Apache HTTP Server
- Apache Tomcat
- Apache Tomcat Native
- curl
- google guava
- Jackson
- JSON-java
- libexpat
- libssh2
- libxml2
- Nimbus JOSE+JWT
- OpenJDK
- OpenSC
- OpenSSL
- Spring Security
- Spring Framework
- zlib

Client and platform updates

Symantec Endpoint Protection Client for Windows

- To reduce the number of URLs that you must list in your proxy or perimeter firewall to communicate with the client, you only need to allow the following URLs.

Client management type	URLs to allow
All clients	• https://liveupdate.symantec.com • https://ent-shasta-rrs.symantec.com • https://sp.cwfservice.net
Cloud-managed clients	• https://us.spoc.securitycloud.symantec.com (North America) • https://eu.spoc.securitycloud.symantec.com (Europe) • https://in.spoc.securitycloud.symantec.com (India)

If you upgrade from 14.3 RU8 and earlier clients, you do not need to add or remove any URLs. Instead, the clients upgrade automatically after LiveUpdate next downloads content.

For information about all the URLs you need to allow, see: [External URLs required for Symantec Endpoint Protection \(SEP\) and Symantec Endpoint Security \(SES\)](#)

- The Windows client is supported on Windows 11 24H2.

Symantec Endpoint Protection Client for Mac

The Symantec Endpoint Protection Client for Mac releases in July 2024.

Symantec Single Agent for Linux

The Symantec Single Agent for Linux releases in July 2024.

Symantec Endpoint Security cloud console

The latest release of the cloud console provides the following enhancements for 14.3 RU9 clients:

- The Symantec Endpoint Security cloud console can send customized notifications to the client user after you manually quarantine a device.
- You can use the **Disable the notification area icon** option to prevent multiple instances of user session processes on the clients that run on a terminal server.
- Threat Defense for Active Directory (TDAD) includes updates such as the ability to cancel a running topology on the clients.

More information

- To learn more about the cloud-based features that are available with a Symantec Endpoint Security license, see: [What's new in Symantec Endpoint Security](#)
- To migrate to the cloud console, see: [Migrating to the SES cloud console](#)

Documentation

The documentation includes the following new topics:

- [Troubleshooting when the Symantec Endpoint Protection Manager blocks you from logging on or upgrading when the server name does not match the server certificate \(14.3 RU9 or later\)](#)
- [Symantec Endpoint Protection Manager detected that the configured replication partner requires certificate verification to be disabled \(14.3 RU9 or later\)](#)
- [How do I block websites with Endpoint Protection \(SEP\)?](#)
- [Blocking or allowing devices using Device Control and Application Control](#)
- [How Application Control works to block devices](#)
- [Deleting a client](#)

To view the database schema, contact Technical Support.

To find the open source attributions file, log on to the Broadcom portal and go to: [Symantec Endpoint Protection Open Source Attributions](#)

System requirements for Symantec Endpoint Protection (SEP) 14.3 RU9

The current version of Symantec Endpoint Protection (SEP) requires the following system requirements.

NOTE

To find system requirements for earlier versions, go to [Related Documents](#) and download the appropriate Release Notes PDF file.

In general, the system requirements for the following are the same as those of the operating systems on which they are supported.

NOTE

An earlier version of Symantec Endpoint Protection Manager may not be able to correctly manage a client with a later version. Issues with content updates and client management may occur. For example, Symantec Endpoint Protection Manager 14.3 RU4 or earlier cannot correctly provide a version 14.3 RU5 client with its version-specific monikers.

The following tables describe the software and hardware requirements for Symantec Endpoint Protection:

- [Symantec Endpoint Protection Manager \(SEPM\) system requirements](#)
- [Symantec Endpoint Protection client for Windows system requirements](#)
- [Symantec Endpoint Protection client for Mac system requirements](#)
- [Symantec Endpoint Protection client for Linux system requirements](#)

Symantec Endpoint Protection Manager (SEPM) system requirements

Table 1: Symantec Endpoint Protection Manager software system requirements

Component	Requirements
Operating system	• Windows Server 2012 • Windows Server 2012 R2 • Windows Server 2016 • Windows Server 2019 • Windows Server 2022 (14.3 RU3 and later) Note: Desktop operating systems are not supported. Note: Windows Server Core edition is not supported.
Web browser	The following browsers are supported for web console access to Symantec Endpoint Protection Manager and for viewing the Symantec Endpoint Protection Manager Help: • Microsoft Edge Chromium Based Browser (14.3 and later) • Microsoft Edge • Mozilla Firefox 5.x through 107 • Google Chrome 113 through 115

Component	Requirements
Database	The Symantec Endpoint Protection Manager includes a default database: • Microsoft SQL Server Express 2014 • Microsoft SQL Server Express 2017 Updating SQL Express 2017 packaged with Endpoint Protection Manager to address vulnerabilities or defects • Sybase embedded database (14.3 MP.x and earlier only) You may instead choose to use a database from one of the following versions of Microsoft SQL Server: • SQL Server 2012 RTM - SP4 (14.3 RU5 and earlier) • SQL Server 2014 RTM - SP3 • SQL Server 2016 SP1, SP2 • SQL Server 2017 RTM • SQL Server 2019 RTM (14.3 and later) • SQL Server 2022 (14.3 RU6 and later) Note: SQL Server databases that are hosted on Amazon RDS are supported. (14.0.1 MP2 and later). Note: If Symantec Endpoint Protection uses a SQL Server database and your environment only uses TLS 1.2, ensure that SQL Server supports TLS 1.2. You may need to patch SQL Server. This recommendation applies to SQL Server 2008, 2012, and 2014. See: Note: TLS 1.2 support for Microsoft SQL Server
Other environmental requirements	• In purely IPv6 networks, the IPv4 stack must still be installed and disabled. If the IPv4 stack is uninstalled, Symantec Endpoint Protection Manager does not work. • Microsoft Visual C++ 2017 Redistributable Package (x64/x86) Note: Note that the required version of Visual C++ is automatically installed during the installation of Symantec Endpoint Protection Manager

Table 2: Symantec Endpoint Protection Manager hardware system requirements

Component	Requirements
Processor	Intel Pentium Dual-Core or equivalent minimum, 8-core or greater recommended Note: Intel Itanium IA-64 processors are not supported.
Physical RAM	2 GB RAM available minimum; 8 GB or more available recommended Note: Your Symantec Endpoint Protection Manager server may require additional RAM depending on the RAM requirements of other applications that are already installed. For example, if Microsoft SQL Server is installed on the Symantec Endpoint Protection Manager server, the server should have a minimum of 8 GB available.
Display	1024 x 768 or larger
Hard drive when installing to the system drive	With a local SQL Server database: • 40 GB available minimum (200 GB recommended) for the management server and database With a remote SQL Server database: • 40 GB available minimum (100 GB recommended) for the management server • Additional available disk space on the remote server for the database

Component	Requirements
Hard drive when installing to an alternate drive	With a local SQL Server database: - The system drive requires 15 GB available minimum (100 GB recommended) - The installation drive requires 25 GB available minimum (100 GB recommended) With a remote SQL Server database: - The system drive requires 15 GB available minimum (100 GB recommended) - The installation drive requires 25 GB available minimum (100 GB recommended) - Additional available disk space on the remote server for the database
Other	An enabled network interface card

If you use a SQL Server database, you may need to make more disk space available. The amount and location of additional space depends on which drive SQL Server uses, database maintenance requirements, and other database settings.

Symantec Endpoint Protection client for Windows system requirements

Table 3: Symantec Endpoint Protection client for Windows software system requirements

Component	Requirements
Operating system (desktop)	For a list of supported operating systems for current and previous releases, see: Windows compatibility with the Endpoint Protection client - Starting in 14.3 RU8, you must have Microsoft Azure Code Signing (ACS) support installed on the client. Microsoft ACS support is available for Windows 8.1 and later only. Upgrading Windows client computers 14.3 RU8 and later with Microsoft Azure Code Signing (ACS) support 14.3 RU6 and later no longer supports computers that run the Microsoft Windows 32-bit operating system. 32-bit computers should run the 14.3 RU5 client.
Operating system (server)	For a list of supported operating systems for current and previous releases, see: Windows compatibility with the Endpoint Protection client To receive the latest SONAR, CIDS, or ERASER content on Windows 7, Windows Server 2008 or Windows Server 2008 R2, see: SONAR 12.3.0, CIDS 17.2.6, and ERASER 119.1.3 Operating System requirements for Windows 7, Windows Server 2008 and 2008 R2
Browser Intrusion Prevention	Browser Intrusion Prevention support is based on the version of the Client Intrusion Detection System (CIDS) engine. See: Supported browsers for Browser Intrusion Prevention in Endpoint Protection

Table 4: Symantec Endpoint Protection client for Windows hardware system requirements

Component	Requirements
Processor (for physical computers)	64-bit processor: 2 GHz Pentium 4 with x86-64 support or equivalent minimum Note: Itanium processors are not supported.
Processor (for virtual computers)	One virtual socket and one core per socket at 1 GHz minimum (one virtual socket and two cores per socket at 2 GHz recommended) Note: The hypervisor resource reservation must be enabled.
Physical RAM	1 GB (2 GB recommended) or higher if required by the operating system
Display	800 x 600 or larger

Component	Requirements
Hard drive	Disk space requirements depend on the type of client you install, which drive you install to, and where the program data file resides. The program data folder is usually on the system drive in the default location C:\ProgramData. Available disk space is always required on the system drive, regardless of which installation drive you choose. Note: Space requirements are based on NTFS file systems. Additional space is also required for content updates and logs.

Table 5: Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to the system drive

Client type	Requirements
Standard	With the program data folder located on the system drive: • 395 MB* With the program data folder located on an alternate drive: • System drive: 180 MB • Alternate installation drive: 350 MB
Embedded / VDI	With the program data folder located on the system drive: • 245 MB* With the program data folder located on an alternate drive: • System drive: 180 MB • Alternate installation drive: 200 MB
Dark network	With the program data folder located on the system drive: • 545 MB* With the program data folder located on an alternate drive: • System drive: 180 MB • Alternate installation drive: 500 MB

* An additional 135 MB is required during installation.

Table 6: Symantec Endpoint Protection client for Windows available hard drive system requirements when installed to an alternate drive

Client type	Requirements
Standard	With the program data folder located on the system drive: • System drive: 380 MB • Alternate installation drive: 15 MB* With the program data folder located on an alternate drive:** • System drive: 30 MB • Program data drive: 350 MB • Alternate installation drive: 150 MB
Embedded / VDI	With the program data folder located on the system drive: • System drive: 230 MB • Alternate installation drive: 15 MB* With the program data folder located on an alternate drive:** • System drive: 30 MB • Program data drive: 200 MB • Alternate installation drive: 150 MB
Dark network	With the program data folder located on the system drive: • System drive: 530 MB • Alternate installation drive: 15 MB* With the program data folder located on an alternate drive:** • System drive: 30 MB • Program data drive: 500 MB • Alternate installation drive: 150 MB

* An additional 135 MB is required during installation.

** If the program data folder is the same as the alternate installation drive, add 15 MB to the program data drive for your total. However, the installer still needs the full 150 MB to be available on the alternate installation drive during installation.

Table 7: Symantec Endpoint Protection client for Windows Embedded system requirements

Component	Requirements
Processor	1 GHz Intel Pentium
Physical RAM	256 MB Note: This figure is for an installation of the Symantec Endpoint Protection embedded client. If you also implement additional features from an integrated solution such as EDR, additional physical RAM is needed.
Hard drive	The Symantec Endpoint Protection Embedded / VDI client requires the following available hard disk space: • Installed to the system drive: 245 MB • Installed to an alternate drive: 230 MB on system drive, and 15 MB on the alternate drive An additional 135 MB is needed during installation. These figures assume that the program data folder is on the system drive. For more detailed information, or for the requirements of the other client types, see the Symantec Endpoint Protection client for Windows system requirements.

Component	Requirements
Embedded operating system	14.3 RU7 and earlier: - Windows Embedded Standard 7 (64-bit) - Windows Embedded POSReady 7 (64-bit) - Windows Embedded Enterprise 7 (64-bit) - Windows Embedded 8 Standard (64-bit) - Windows Embedded 8.1 Industry Pro (64-bit) - Windows Embedded 8.1 Industry Enterprise (64-bit) - Windows Embedded 8.1 Pro (64-bit) Starting in 14.3 RU8, you must have Microsoft Azure Code Signing (ACS) support installed on the client, which is not available for Windows Embedded.
Required minimum components	- Filter Manager (FltMgr.sys) - Performance Data Helper (pdh.dll) - Windows Installer Service
Templates	- Application Compatibility (Default) - Digital Signage - Industrial Automation - IE, Media Player, RDP - Set Top Box - Thin Client The Minimum Configuration template is not supported. The Enhanced Write Filter (EWF) and the Unified Write Filter (UWF) are not supported. The recommended write filter is the File Based Write Filter (FBWF) installed along with the Registry Filter.

Symantec Endpoint Protection client for Mac system requirements

Table 8: Symantec Endpoint Protection client for Mac system requirements

Component	Requirements
Processor/Chip	64-Bit Intel Core 2 Duo and later Apple M1 chip (as of 14.3 RU2) Apple M2 chip (as of 14.3 RU5)
Physical RAM	2 GB of RAM
Hard drive	1 GB of available hard disk space for the installation Running the Symantec Endpoint Protection Installer on a case-sensitive file system is unsupported.
Display	800 x 600
Operating system	For a list of supported operating systems for current and previous releases, see: MacOS and OSX compatibility for Endpoint Protection
Internet connectivity	Requires access to an internet host. See: Use Apple products on enterprise networks

Symantec Single Agent for Linux system requirements

Table 9: Symantec Single Agent for Linux system requirements

Component	Requirements
Hardware	• Physical: Intel Pentium 4 (2 GHz) or equivalent with 2 cores, minimum (4 cores recommended) • Virtual: One virtual socket with 2 cores, minimum (4 cores recommended) • RAM: 512MB of available RAM minimum (4GB recommended) • 2 GB available disk space if <code>/var</code>, <code>/opt</code>, and <code>/tmp</code> share the same filesystem or volume • 1 GB available disk space in each <code>/var</code>, <code>/opt</code>, and <code>/tmp</code> if on different volumes An additional 5 GB of disk space is recommended in <code>/opt</code> if you enable any Symantec Endpoint Detection and Response features.
Operating system	Supported operating systems: • Amazon Linux 2023 • Amazon Linux 2 • CentOS Linux 6, 7, 8* • CentOS Stream is not supported as of SEP 14.3 RU7 • Debian 9, 10 (14.3 RU2 and later) • Oracle Enterprise Linux 6, 7, 8* • Rocky Linux 8, 9 • Red Hat Enterprise Linux 6, 7, 8*, 9 Linux 6.x is not supported for a dual-managed single agent (e.g., DCS and SEP Linux). A standalone SEP Linux agent (SEPM managed or Cloud managed) is supported on RHEL 6.x. • SuSE Linux Enterprise Server 12.x, 15.x • Ubuntu 16.04 LTS, 18.04 LTS, 20.04 LTS, 22.04 LTS (14.3 RU6 and later) * If you are running RHEL/OEL/CentOS 8.x with FIPS mode enabled in dual-managed mode with a DCS agent, the agent is unable to communicate with DCS Server. Communication is restored when you disable FIPS and restart the system. For more information, and for lists of supported minor Linux OS versions, see: Supported kernels of Symantec Linux Agent Supported operating systems for version 14.3 MP1 and earlier: • Amazon Linux and Linux 2 • CentOS 6U3 - 6U9, 7 - 7U7, 8; 32-bit and 64-bit • Debian 6.0.5 Squeeze, Debian 8 Jessie; 32-bit and 64-bit • Fedora 16, 17; 32-bit and 64-bit • Oracle Linux (OEL) 6U2, 6U4, 6U5, 6U8; 7, 7U1, 7U2, 7U3, 7U4 • Red Hat Enterprise Linux Server (RHEL) 6U2 - 6U9, 7 - 7U8, 8-8U2 • SUSE Linux Enterprise Server (SLES) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12, 12 SP1 - 12 SP3, 64-bit • SUSE Linux Enterprise Desktop (SLED) 11 SP1 - 11 SP4, 32-bit and 64-bit; 12 SP3, 64-bit • Ubuntu 12.04, 14.04, 16.04, 18.04 (as of 14.3); 32-bit and 64-bit For a list of supported operating system kernels for previous releases, see: List of Linux Distributions and Kernels with Precompiled Auto-Protect Drivers/Modules for Symantec Endpoint Protection for Linux 14.x

Component	Requirements
Dependencies	You must install the following list of dependent packages and libraries on the computer where you create the installation package. These packages and libraries are specifically checked by the installation process. This list is cumulative per release. Core system packages: • checkpolicy: SELinux policy compiler. • policycoreutils-python: SELinux policy core python utilities. • upstart: An event-driven init system. • bash: The GNU Bourne Again shell (bash). • dmidecode: Retrieves SMBIOS/DMI table information. • sed: A GNU stream text editor. • gzip: The GNU data compression program. • tar: The GNU file archiving program. • gawk: The GNU version of the awk text processing utility. • grep: The GNU versions of grep pattern matching utilities. • findutils: The GNU versions of find utilities (find and xargs). • coreutils: The GNU core utilities - a set of commonly used utility applications. • module-init-tools: Kernel module management utilities. • util-linux-ng: A collection of basic system utilities. • filesystem: The basic directory layout for a Linux system. • shadow-utils: Utilities for managing accounts and shadow password files. • zip: A file compression and packaging utility compatible with PKZIP. Dependent libraries: • auditd: audit daemon generates log entries to record information. • openssl: The OpenSSL toolkit (x86_64). <i>(Not needed from 14.3 RU4 onwards)</i> • glibc: The GNU libc libraries (x86_64). • libstdc++: The GNU Standard C++ Library v4 (x86_64). • libgcc: GCC version 4.0 shared support library (x86_64). • pam: PAM Authentication Libraries (64bit libpam.so). • zlib: A Massively Spiffy Yet Delicately Unobtrusive Compression Library (x86_64). • libacl: Utilities to administer Access Control Lists (x86_64). • at: Job spooling tools. • libelf: Libraries for creating custom tools for manipulating ELF programs and shared libraries. • libdw1: Library providing access to DWARF debug information stored inside ELF files.
Graphical desktop environments	You can use the following graphical desktop environments to view the Symantec Endpoint Protection for Linux client: • KDE • Gnome • Unity Symantec Agent for Linux 14.3 RU1 does not have a graphical user interface.

Component	Requirements
Older environmental requirements	14.3 RU1 to 14.3 RU3: • OpenSSL 1.0.2k-fips or later 14.3 MP1 and earlier: • Glibc Any operating system that runs glibc earlier than 2.6 is not supported. • net-tools or iproute2 Symantec Endpoint Protection uses one of these two tools, depending on what is already installed on the computer. • Developer tools Auto-compile and the manual compile process for the Auto-Protect kernel module require that you install certain developer tools. These developer tools include gcc and the kernel source and header files. For details on what to install and how to install them for specific Linux versions, see: Manually compile Auto-Protect kernel modules for Endpoint Protection for Linux • i686-based dependent packages on 64-bit computers Many of the executable files in the Linux client are 32-bit programs. For 64-bit computers, you must install the i686-based dependent packages before you install the Linux client. If you have not already installed the i686-based dependent packages, you can install them by command line. This installation requires superuser privileges, which the following commands demonstrate with <code>sudo</code>: – For Red Hat-based distributions: <code>sudo yum install glibc.i686 libgcc.i686 libX11.i686 libnsl.i686</code> – For Debian-based distributions: <code>sudo apt-get install ia32-libs</code> – For Ubuntu-based distributions: <pre>sudo dpkg --add-architecture i386 sudo apt-get update sudo apt-get install gcc-multilib libx11-6:i386</pre>

More information

[Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security](#)

Known issues and workarounds for Symantec Endpoint Protection (SEP)

The items in this section apply to this release of Symantec Endpoint Protection.

NOTE

The Issue column displays the version number when the issue appears. For example, [14.3 RU1] means that the issue applies to version 14.3 RU1 and later. When these issues are fixed, they appear in the fix-it notes. See:

[Versions, system requirements, release dates, notes, and fixes for Symantec Endpoint Protection and Endpoint Security](#)

Known issues in 14.3 RU9

Table 10: Version 14.3 RU9

Issue ID	Description	Workaround
INFODEVSEP-70	The Symantec Endpoint Protection client 14.3 RU9 is incompatible with the on-premises Symantec EDR 4.9 and earlier. This issue is caused by the fewer number of URLs that you must allow for 14.3 RU9 clients. [14.3 RU9] External URLs required for Symantec Endpoint Protection (SEP) and Symantec Endpoint Security (SES)	This issue is fixed in Symantec EDR version 4.10, which is targeted to release in June 2024. If your environment includes Symantec EDR, do one of the following tasks: - Wait to upgrade to SEP 14.3 RU9 until Symantec EDR 4.10 is released and then upgrade them both at the same time. - Upgrade to SEP 14.3 RU9 at any time and install the Symantec EDR 4.9 patch.
INFODEVSEP-54	The following error message appears every 24 hours on the Admin > Servers page: The enrolled Symantec Endpoint Protection Manager did not replicate Adaptive Protection events with the remote site. [{_}sitename{_] } This issue occurs when the Symantec Endpoint Protection Manager is enrolled in the cloud console and has not replicated with its replication partner for at least two cycles. The replication partner usually does not replicate when the primary site is offline. [14.3 RU9]	You must successfully replicate between the sites.

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU9](#)

Known issues in 14.3 RU8**Table 11: Version 14.3 RU8**

Issue ID	Description	Workaround
SEP-85508	When using Live Shell in the client or cloud console, some text may be displayed incorrectly. Characters may be replaced with the Unicode replacement character (diamond with question mark) or other unexpected characters. [14.3 RU8 and earlier] See: Live Shell in ICDm displays a Unicode replacement character or other unintelligible characters	Upgrade to 14.3 RU9
ESMAC-7043	File Activity [8003] events are no longer sent by Mac agents connected to Symantec Endpoint Detection & Response (EDR). [14.3 RU8] For Mac agents reporting to the cloud console in Symantec Endpoint Security (SES), trigger a Full Dump to view 8003 events.	On-premise Mac agents configured to send events to EDR 4.8 and earlier will be enhanced in a future EDR release.

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU8](#)**Known issues in 14.3 RU7****Table 12: Version 14.3 RU7**

Issue ID	Description	Workaround
SEP-82895	After you restore a file that the SEP client quarantined, and then run an Auto-Protect scan on the restored file, the SEP client does not detect the virus. [14.3 RU7] This issue occurs when the Coexist with Windows Defender option is enabled and you restore a file from the quarantine. Windows Defender blocks Auto-Protect from detecting viruses in restored files, but can make its own detection.	1. Disable the Coexist with Windows Defender option. 2. Restore any files that have been in the quarantine and cleaned. 3. Reenable Coexist with Windows Defender.
SEP-82580	After disabling the Coexist with Windows Defender option within a Virus and Spyware Protection policy, Windows Defender is not disabled as expected. [14.3 RU7] When disabling co-exist mode, the Endpoint Protection/Security Agent is unable to disable Windows Defender if Windows Defender Tamper Protection is enabled because Windows Defender Tamper Protection blocks the action.	To allow the Endpoint Protection/Security agent to disable Windows Defender when disabling coexistence mode, Windows Defender Tamper Protection must be disabled. Alternatively, Windows Defender can be disabled manually. See: Windows Defender is not disabled when turning off coexistence mode in Endpoint Protection
SEP-83786	The Windows client Troubleshooting > Web and Cloud Access Protection page shows the following status message: Warning: Using CTCv1 (missing enrollment token) [14.3 RU7]	See: Warning: "Using CTCv1 (missing enrollment token)" warning in Web and Cloud Access Protection on SEP client 14.3 RU7 or later

[New fixes and component versions in Symantec Endpoint Protection 14.3 RU7](#)

Known issues in 14.3 RU6**Table 13: Version 14.3 RU6**

Issue ID	Description	Workaround
SEPLINUX-1468	Monitoring of file system activity on the NFS file system is not yet supported for the EDR feature.	In 14.3 RU6 and later, only File rename and delete events are captured.
SEP-81247	If you remove the Advanced Download Protection feature from the Windows client, the SEPM still shows that the Advanced Download Protection feature is enabled. [14.3-RU6] Download Protection uses the IPS to retrieve information about files being accessed. If you remove Advanced Download Protection, you are not removing the IPS. Therefore, the Clients page > Clients tab still shows the Download Protection Status column as Enabled - Advanced Protection .	You can install the Basic Download Protection and Intrusion Prevention features, which are the same as Advanced Download Protection .

New fixes and component versions in Symantec Endpoint Protection 14.3 RU6**Known issues in 14.3 RU5****Table 14: Version 14.3 RU5**

Issue ID	Description	Workaround
SEP-79993	When you upgrade from a 14.3 RU4 client to a 14.3 RU5 client and import a file fingerprint list that uses SHA-256 fingerprints, the system lockdown list does not correctly block applications. This issue occurs because the 14.3 RU5 and later client uses the 14.3 RU4 version of the <code>sysfer</code> and <code>sysplamt</code> services.	Restart the 14.3 RU5 and later client after you upgrade from 14.3 RU4.
SEP-80222	The Status page on a 14.3 RU4 Windows client that a Symantec Endpoint Protection Manager 14.3 RU5 manages shows the following error: "Proactive Threat Protection is malfunctioning." [14.3 RU5]	The issue is caused because in 14.3 RU4 and earlier, SONAR depended on Auto-Protect being enabled. In 14.3 RU5, SONAR is no longer disabled when Auto-Protect is disabled. Therefore, when an 14.3 RU4 client receives the Virus and Spyware Protection policy from a Symantec Endpoint Protection Manager 14.3 RU5, SONAR is enabled but the client still shows the error. Security agents previous to 14.3 RU5 warn Proactive Threat Protection is not functioning when Auto-Protect is disabled by policy and locked
SEPLINUX-1502	In SEP 14.3 RU4 and earlier, when executing the forensic command to the Linux agent, the command would remain in the "In Progress" state for an extended period. [14.3 RU5]	The following are workarounds for this issue: 1. Cancel the command from the Symantec Endpoint Security (SES) console and re-issue it. 2. Allow the command to time out on the server. 3. Log on to the Agent system and restart the CAFDaemon.

Issue ID	Description	Workaround
SEPLINUX-1472	When running the Intelligent Updater script on RHEL9, a message appears on the console indicating that the "uncompress" executable is not present on the system. [14.3 RU5]	As of RHEL9, <code>ncompress</code> is deprecated. If you are running RHEL9, you must obtain <code>ncompress rpm</code> and install it on your system for the Intelligent Updater to work. Intelligent Updater is not supported on RHEL9

Known issues in 14.3 RU4

Table 15: Version 14.3 RU4

Issue ID	Description	Workaround
SEP-77602	Attack Surface Reduce Log - Hardening Logs size ignores policy setting and is always 5 MB or larger. [14.3 RU4] In Symantec Endpoint Protection (SEP) agent version 14.3 RU4, the Attack Surface Reduction log maximum size is 5 MB (5,120 kb), even though the Security and Risk Logs Maximum Size in Client Log settings is configured to less than 5,120 KB. If the value is larger than 5,120 KB, then it adheres to the value. This issue occurs because the Attack Surface Reduction log (ASRman.log) contains more events than other Security and Risk logs (such as avman.log, tdadman.log). So a larger default size is required to retain sufficient events.	The 5 MB minimum is a temporary measure until a configurable value for Attack Surface Reduction is added to the Client Log settings. Until then, the log will either be 5mb or match the value that is configured in the Security and Risk log (whichever is larger). Attack Surface Reduce Log - Hardening Logs size ignores policy setting and is always 5MB or larger
	Symantec Endpoint Protection (SEP) 14.3 RU4 and older clients show the message <code>Component is Malfunctioning</code> as their SONAR status if Auto-Protect is disabled. The clients that show this message are managed by a Symantec Endpoint Protection Manager version 14.3 RU5 or later. For 14.3 RU4 and later clients, SONAR is not completely malfunctioning when Auto-Protect is disabled, but there is some efficacy impact on the SONAR component when Auto-Protect is disabled.	Make sure that you keep Auto-Protect enabled.
SEPLINUX-1488	Intelligent Updater fails to restart AMD service on RHEL6. [14.3 RU4]	If you are running RHEL6, you must restart the <code>sisamdagent</code> service (service <code>sisamdagent</code> restart) after running the Intelligent Updater script.
SEPLINUX-483	Linux agent does not communicate with DCS server. [14.3 RU4] If you are running RHEL/OEL/CentOS 8.x with FIPS mode enabled in dual-managed mode with a DCS agent, the agent is unable to communicate with DCS Server.	Communication is restored when you disable FIPS and restart the system. Dual managed DCS and SEP Linux are not supported.

[New fixes and components for Symantec Endpoint Protection 14.3 RU4](#)

Known issues in 14.3 RU3**Table 16: Version 14.3 RU3**

Issue ID	Description	Workaround
SEP-72814	Endpoint Protection (SEP) 14.2 RU1 MP1 and earlier clients do not honor the Upgrade Schedule settings in a Client Upgrade Policy. [14.3 RU3]	For more information, see: Endpoint Protection 14.3 RU1 MP1 and older clients not following Client Upgrade Policy
SEPM-433	When you click the Advanced Security page, a blank page may appear with the following error message: File or Directory Was Not Found - The requested file or directory could not be located. [14.3 RU3 with a Symantec Endpoint Security Complete license] If the Symantec Endpoint Protection Manager and the Data Center Security client are installed on the same computer, LiveUpdate is not able to display the Advanced Security page content, and you cannot enroll the SEPM in the cloud console.	Configure the DCS prevention policy: 1. In the Symantec Data Center Security (DCS) Server Manager console, open the Prevention policy that is applied to the DCS client. 2. Click Application Rules. 3. In the Application Rules panel, select the Symantec Endpoint Protection entry. 4. Click Edit. 5. Add the following rules: – Program path: %%-HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM\JavaLaunchTool\JavaEXE%% – Program path: %%-HKEY_LOCAL_MACHINE\SOFTWARE\Symantec\Symantec Endpoint Protection\SEPM\JavaLaunchTool\JavaW%% 6. Enter a rule name and description as SEPM console. 7. Keep the remaining fields of the rule blank. 8. Save the policy and apply it to the DCS client. 9. In a Run command, stop and restart the Symantec Endpoint Protection Manager services as follows: – net stop semsrv – net stop semapisrv – net stop semwebsrv – net stop semlaunchsrv – net start semsrv – net start semapisrv – net start semwebsrv – net start semlaunchsrv
	Endpoint Protection 14.3 RU3 Web and Cloud Access Protection log reports the Windows 10 operating system as Windows 11. [14.3 RU3] In the SEP client Web and Cloud Access Protection log, the log shows the operating system as Windows 10 when the client is installed on a Windows 11 device. On the client console, click Web and Cloud Access Protection > Options > View Logs.)	

Issue ID	Description	Workaround
SEP-75086	Microsoft Edge browser and the Google Chrome browser are not able to launch after the Validate image dependency integrity mitigation technique is applied to the Windows 10 or 11 operating system. [14.3 RU3] One of the mitigation techniques that Microsoft Edge uses to protect the Windows operating system is the Validate image dependency integrity technique. For Windows 10 or 11 computers that run the Symantec Endpoint Protection clients versions 14.2 RU2 MP1 or later, if this option is enabled, both Microsoft Edge and the Google Chrome web browsers do not launch.	To ensure that Microsoft Edge launches, disable the Validate image dependency integrity technique. For more information on mitigation techniques for Microsoft Edge, see: Customize exploit protection See also: Microsoft Edge and Google Chrome do not open if "Validate image dependence integrity" mitigation technique is applied and SEP 14.2 RU2 MP1 or later is installed
SEP-73327	You must restart the rebootless Windows client to obtain the latest EDR events. [14.3 RU3] To make more ETW events available in 14.3 RU3, you must restart the Symantec Endpoint Protection client. You must restart the client in the following situations: • If EDR is enabled and you update the client to RU3. • 14.3 RU3 is already installed and you enable or disable EDR. You must restart the client to enable or disable the newly added events.	See: A restart may be required to begin seeing some ETW events with EDR and SEP 14.3 RU3
SEP-74510	Unexpected server error when logging into Endpoint Protection Manager and clients are no longer communicating after a system time change. [14.3 RU3] If you set the system clock back to a previous date and/or time, the following error may occur: • After you log on to the Symantec Endpoint Protection Manager, an Unexpected Server Error appears. • The clients do not communicate with SEPM, which reports a 503 error.	• Manually restart the SEPM services. • Wait until the date/time on the system passes the original time on the system before you set it back.
ESMAC-3339	On Mac client, VNC/screen sharing connectivity is lost if Vulnerability Protections are disabled or enabled. [14.3 RU3] Issue is observed on MacOS 12 and MacOS 11.4 (ARM).	

[New fixes and components for Symantec Endpoint Protection 14.3 RU3](#)

Known issues in 14.3 RU2

Table 17: Version 14.3 RU2

Issue ID	Description	Workaround
SEP-72531	The following error message appears: Symantec Endpoint Protection version 14.3 RU2 for Win64bit is the latest package. You cannot delete it. [14.3 RU2]	You cannot delete the Client Install Package when packages from multiple builds appear in the Symantec Endpoint Protection Manager. As of 14.3 RU2, LiveUpdate can download multiple client installation packages with a different build number, which appear in the Admin page > Install Packages > Client Install Package table.
SEP-72490	AutoUpgrade fails if you use the Upgrade to English if currently installed language is unsupported option to upgrade clients with an unsupported language to English. [14.3 RU2] This issue is caused because the client language uses the language of the supported operating system (in this case, Japanese). AutoUpgrade expects to use the supported language and not English.	Try the AutoUpgrade again and turn off the Upgrade to English if currently installed language is unsupported option.
	When exporting a client installation package from a 14.3 RU2 Symantec Endpoint Protection Manager (SEPM), the following warning message appears: "The client installation package does not have content." [14.3 RU2]	This issue occurs when communication between the Symantec Endpoint Protection Manager and the console being used to export the package is disrupted. See: "The client installation package does not have content." warning when exporting an installation package from the Endpoint Protection Manager
SEP-72292	An error appears when importing the most recent client installation packages into an older version of Symantec Endpoint Protection Manager. [14.3 RU2]	Symantec Endpoint Protection 14.3 RU2 clients cannot be managed by a 14.3 RU1 MP1 or earlier Symantec Endpoint Protection Manager.
SEP-70385	After upgrading a Symantec Endpoint Protection Manager to 14.3 RU2, php-cgi.exe crashes with an error in the event viewer. [14.3 RU2] This issue occurs with the 17.4.1.1 version of the Microsoft ODBC Driver for SQL Server in 14.3 RU2 clients.	Download and install the 17.7.2 version of the Microsoft ODBC Driver for SQL Server on Windows. Release Notes for Microsoft ODBC Driver for SQL Server on Windows php-cgi.exe crash occurs on Endpoint Protection Manager after upgrading to 14.3 RU2
	If you upgrade the Symantec Endpoint Protection Manager from 14.3 RU1 to a later version, you may see the following notifications: The client computer has been renamed [14.3 RU2] If upgrading from Symantec Endpoint Protection Manager 14.3 RU1 or earlier to 14.3 RU2 or later, administrators may start receiving The client computer has been renamed notifications. This issue is applicable only to Mac clients.	"The client computer has been renamed" notifications may appear after upgrading to Symantec Endpoint Protection Manager 14.3 RU2
	Custom names may prevent the firewall policy from updating during an upgrade to 14.2 or later. [14.3 RU2] For an upgrade to Symantec Endpoint Protection 14.2 or later, firewall policies cannot incorporate the changes for IPv6 if you changed some default names. The default names include the names of default policies and default rule names. If the rules cannot be updated during the upgrade, the IPv6 options do not appear. Any new policies or rules that you create after the upgrade are not affected.	If possible, revert any changed names back to the default. Otherwise, ensure that any custom rules that you added to a default policy do not block IPv6 communication in any way. Ensure the same for any new policies or rules that you add.

Issue ID	Description	Workaround
	Rosetta may block the Mac agent installation on Apple Silicon (M1) devices with the following error: "This version of Symantec Agent for Mac is not supported on Apple M1 chip." [14.3 RU2]	For more information, see: Rosetta may block the Mac client installation on Apple Silicon (M1) devices

Known issues in 14.3 RU1

Table 18: Version 14.3 RU1

Issue ID	Description	Workaround
SEP-67175	Some EDR events do not appear on the client. [14.3 RU1]	The Symantec Endpoint Protection client must run Windows 10 build 14393 or later to collect Symantec EDR Event Tracing for Windows (ETW) events.
SEP-68700	The Web and Cloud Access Protection feature has some limitations. [14.3 RU1] • The Symantec Cloud Secure Web Gateway (Cloud SWG) was delivered on IPv4 and not IPv6. • The tunnel redirection method: – Runs on Windows 10 x64 version 1703 and later (Semi-Annual Servicing Channel), Windows 11, SEP Mobile, and the Mac. [SEP-67927] – Does not support HVCI-enabled Windows 10 64-bit devices. [SEP-67648] – Redirects outbound traffic from the Symantec Endpoint Protection client to the Cloud SWG before it gets evaluated by either the client's firewall or the URL reputation rules. Instead, that traffic is evaluated against the WSS firewall and the URL rules. For example, if a SEP client firewall rule blocks google.com and a WSS rule allows google.com, the client allows users to access google.com. Inbound local traffic to the client is still processed by the Symantec Endpoint Protection firewall. [SEP-67488] – SAML authentication replaced the Captive Portal to authenticate users and groups on the Symantec Endpoint Protection client. – If a client computer connects to the WSS using the tunnel method and hosts virtual machines, each guest user must install the SSL certificate provided in the Cloud SWG portal. – Traffic for local network like your home directory or Active Directory authentication is not redirected. – Is not compatible with the Microsoft DirectAccess VPN.	
SEP-68965	Duplicate client enrollment entries after the upgrade from 14.2.x to 14.3 MP1 and later. [14.3 RU1] Upgrading the Symantec Endpoint Protection clients from 14.2.x to 14.3 MP1 and later creates duplicate agent enrollment entries for these clients on the Clients page in Symantec Endpoint Protection Manager.	There is no functional impact and you can continue working with the new entries for 14.3 RU1 clients. Symantec Endpoint Protection Manager removes older agent entries.

Issue ID	Description	Workaround
SEP-75205	When you upgrade from the default SEPM embedded database to a Microsoft SQL Server Express database, the following error may appear: The specified password does not meet strong password requirements. [14.3 RU1] This error occurs because the SQL Server Express password requirements use the Windows password requirements. If the default database password requirements are more stringent than what the default SEPM installation script uses, this error occurs.	See: While upgrading a SEPM embedded database to 14.3 RU1 the error "The specified password does not meet strong password requirements"
SEP-69125	A Symantec Endpoint Protection Manager in a dark network downloads old Client Intrusion Detection System (CIDS) content to new clients because LiveUpdate does not run during an upgrade. [14.3 RU1] When a 14.3 RU1 or later Symantec Endpoint Protection Manager cannot access either the Internet or a LiveUpdate Administrator (LUA) server, it keeps old, incompatible content in its cache. This old content is normally delivered to the new clients. To update the content in the management server's cache, you manually download certified virus definitions and CIDS .jdb files.	To make sure that the new clients do not get old content, manually install a CIDS .jdb file on SEPM before you install new clients or upgrade old clients. See: Download .jdb files to update definitions for Endpoint Protection Manager
	You cannot log on to Symantec Endpoint Protection Manager (SEPM) when the network interface card is disabled. [14.3 RU1] If after you install Symantec Endpoint Protection Manager, you cannot log on to the console and the following error message appears: <code>Unexpected server error</code> This issue may occur if the computer's network interface card is disabled when you installed the SEPM, which keeps the server certificate from being generated. This issue occurs when certificate validation fails during installation because the SEPM installer is unable to get the host name if all network cards are disabled. The . . . \apache\conf\server.crt file shows the Issued to and Issued by fields as blank.	Enable at least one network adapter, uninstall the SEPM, then reinstall the SEPM. See: Unexpected server error at SEPM login if it was installed on a server without an enabled NIC
SEP-68670	When you uninstall SEPM and use the option to remove the default database and leave the SQL Server Express instance, the following error appears: "An error occurred while trying to connect to the database server". [14.3 RU1] If you uninstall the Symantec Endpoint Protection Manager and select the Remove only the DB and leave the SQL Server Express instance installed with SEPM option, you may see the following error: "An error occurred while trying to connect to the database server." This issue occurs after you add the credentials for the default user DBA and may be related to user privileges.	Perform the uninstallation by running the SEPM setup.exe file and clicking the Remove only the DB and leave the SQL Server Express instance installed with SEPM option during uninstallation.
SEP-70996	Upgrade installation package that is used for clean installation installs the default feature set. [14.3 RU1 MP1 and earlier] If you create an upgrade installation package with Maintain existing client features when updating option checked, and use this package to do a clean installation, the default feature set is installed on your client device.	If you want to install a custom feature set, you must create a separate installation package for the clean installation.
SEP-72481	If you automatically upgrade a client with an unsupported language to English, the client continues to display the date settings for definitions in English. [14.3 RU1 and later]	Uninstall the legacy client and manually install a new English client installation package. In addition, a fix is expected for clients that are upgraded automatically.

New fixes and components for Symantec Endpoint Protection 14.3 RU1 MP1

New fixes and components for Symantec Endpoint Protection 14.3 RU1

Known issues in 14.3 and earlier

Table 19: Versions 14.3.x and earlier

Issue ID	Description	Workaround
SEP-61473	A SQL Server upgrade from version 2017 to version 2019 fails with FIPS mode enabled. [14.3] You may see the error: "The following error has occurred. An error occurred while installing the extensibility feature with the error message: AppContainer Creation Failed with error message NONE state. This implementation is not part of the Windows Platform FIPS validated cryptographic algorithms." This issue occurs if you have a FIPS-enabled Symantec Endpoint Protection Manager 14.3 and you upgrade from the Microsoft SQL Server 2017 through 2019.	Disable FIPS at the operating system level: 1. In C:\ProgramData\Microsoft\Windows\Start Menu\Programs\Administrative Tools, click Local Security Policy > Local Policies > Security Options, and disable System cryptography: Use FIPS compliant algorithms for encryption, hashing and signing 2. Upgrade from SQL Server version 2017 to version 2019. 3. After SQL Server upgrades successfully, re-enable FIPS. For more information, see: SQL upgrade from 2017 to 2019 fails with FIPS mode enabled
SEP-61106	The Symantec Endpoint Protection Manager remote console no longer supports the 32-bit Windows platform. [14.3] In 14.3 and later, you cannot log on to the Symantec Endpoint Protection Manager remote console if you run a 32-bit version of Windows. The Oracle Java SE Runtime Environment no longer supports 32-bit versions of Microsoft Windows.	If you see the following message, log on to Symantec Endpoint Protection Manager locally: "This version of C:\Users\Administrator\Downloads\Symantec Endpoint Protection Manager Console\bin\javaw.exe is not compatible with the version of Windows that you are running. Check your computer's system information and then contact the software publisher."
SEP-60396	"Failed to install Microsoft Visual C++ Runtime" error appears while you install the Symantec Endpoint Protection Manager. [14.3] You may see the following error while installing the Symantec Endpoint Protection Manager on Windows 2012 R2: "Failed to install Microsoft Visual C++ Runtime"	To work around this issue, activate Windows and install the Windows updates. The Windows update installs the Visual C++ 2017 redistributable, which is a prerequisite for the Symantec Endpoint Protection Manager 14.3 installation on Windows 2012 R2.
	Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows. [14.3] After you upgrade to or install a Symantec Endpoint Protection Manager version 14.3 that is enrolled in the cloud console, the management server no longer uploads logs successfully to the cloud. In the uploader.log you may see the following error: <SEVERE> WinHttpRequest: 12175: A security error occurred	This issue is caused by a missing Microsoft update that provides support for TLS 1.1 and 1.2. To solve the issue, install Microsoft update: KB3140245. For more information, see: Update to enable TLS 1.1 and TLS 1.2 as default secure protocols in WinHTTP in Windows

Issue ID	Description	Workaround
	The standalone Symantec WSS Agent blocks the Symantec Endpoint Protection client installation if you install SEP on the same computer as the WSS Agent. The Web and Cloud Access Protection component uses the same files as the standalone Symantec WSS Agent (WSSA). Web and Cloud Access Protection is installed by default in both Symantec Endpoint Protection and the Symantec Endpoint Security cloud console. If Web and Cloud Access Protection is installed on an endpoint, WSSA cannot be installed. Similarly, if WSSA is installed, Web and Cloud Access Protection does not install.	You can remove the Web and Cloud Access Protection feature from existing endpoints without having to uninstall the whole client by using one of the following methods: - In Symantec Endpoint Protection Manager, create a Client Install Feature Set that does not include Web and Cloud Access Protection and apply it to the endpoints. See: Add or remove features to existing Endpoint Protection clients - The following command-line option uses the client installation file to remove Web and Cloud Access Protection: <code>setup.exe /s /v" REMOVE=NTR /qn"</code>
SEP-61175/61403	The Symantec Endpoint Protection 14.3 Windows client installation may fail unless you first install SHA-2 support. [14.3] If you run legacy operating system versions (Windows 7 RTM or SP1, Windows Server 2008 R2 or R2 SP1 or R2 SP2), you are required to have SHA-2 code signing support that is installed on your devices for Windows updates that are released on or after July 2019. Without SHA-2 support, the Windows client installation sometimes fails. The installation may fail whether you install clients for the first time or automatically upgrade from a previous release. If you want to run Windows Update on such machines you must pre-install the relevant patches too.	To get Microsoft enforced SHA-2 code signing support, see: 2019 SHA-2 Code Signing Support requirement for Windows and WSUS Symantec Endpoint Protection 14.3 Windows client may fail to install unless SHA-2 support is installed
CDM-42467	Allow URLs in Symantec Endpoint Security if you use the hybrid management option for a proxy server or a perimeter firewall. [14.3] With Broadcom's acquisition of Symantec Enterprise Security, the URLs for client-to-cloud communication changed in 14.2.2.1. This issue occurs when the Symantec Endpoint Protection Manager is enrolled in the Symantec Endpoint Security cloud console.	You must upgrade your clients to version build 14.3 MP1 (14.3.1169.0010) or later in the following situations. - You use Symantec Endpoint Security to manage your clients and policies when your on-premises Symantec Endpoint Protection Manager domains are enrolled in the cloud console. - You use proxy servers. You allow the URLs in either fully cloud-managed or hybrid-managed agents in your proxy server and/or perimeter firewall. See: External URLs required for Endpoint Protection (SEP) and Endpoint Protection (SES) Converting the Symantec Endpoint Protection clients from on-premises managed to cloud-managed

Issue ID	Description	Workaround
	"Deployment in progress" still appears in Symantec Endpoint Protection Manager after the client receives an updated policy for Endpoint Threat Defense for AD. [14.2 RU1 MP1 and later]	This behavior is expected. Endpoint Threat Defense for AD 3.3 policies are only supported on the client as of version 14.2 RU1 MP1. You apply a policy for Symantec Endpoint Threat Defense for Active Directory 3.3 to a group. This group contains some clients that run Symantec Endpoint Protection 14.2 RU1 or earlier. These clients receive and apply the policy as expected, but the status in the Symantec Endpoint Protection Manager continues to show the message Deployment in progress.
	Microsoft Edge unexpectedly allows PDF downloads with Hardening enabled. [14.2 RU1 MP1 and later] With Application Hardening enabled in the Symantec Endpoint Protection client, you are unexpectedly able to download PDF files if you use the Microsoft Edge browser. The prevention of the download of PDF files works as expected with other browsers.	A fix for this issue is planned for a future release.

[New fixes and components for Symantec Endpoint Protection 14.3 MP1](#)

[New fixes and components for Symantec Endpoint Protection 14.3](#)

Documentation

You can find documentation on the Broadcom [Symantec Security Tech Docs Portal](#).

To find the Endpoint Protection documentation, click the **Symantec Security Software** tab, then click **Endpoint Security and Management > Endpoint Protection**.

To find a PDF file, go to the [Related Documents](#) page.

To find the Symantec Endpoint Protection Manager database schema, contact Support.

Supported and unsupported upgrade paths to the latest version of Symantec Endpoint Protection

Generally, for Symantec Endpoint Protection versions earlier than the latest version, every version on the list before it is supported. However, you should confirm by referring to the release notes for your specific version. See:

[Release versions, notes, new fixes, and system requirements for Endpoint Security and all versions of Endpoint Protection](#)

See also: [Upgrade best practices for Endpoint Protection 14.x](#)

Symantec Endpoint Protection client for Windows

The following versions of the Symantec Endpoint Protection Windows client can upgrade directly to the current version:

- All releases of 14.x, 14.2.x, and 14.3.x

Symantec Endpoint Protection client for Mac

The following versions of the Symantec Endpoint Protection client for Mac can upgrade directly to the current version:

- All releases of 14.x, 14.2.x, and 14.3.x (14.3 RU7 was not released).
The Symantec Endpoint Protection client for Mac was not updated for 14.0.1 MP2.

Symantec Single Agent for Linux

NOTE

As of version 14.3 RU1, the Linux client installer detects and uninstalls earlier versions of the Linux client, and then performs a fresh install of the new client. Old configurations are not retained.

The following versions of the Symantec Endpoint Protection client for Linux can upgrade directly to current version:

- All releases of 14.x, 14.2.x, and 14.3.x (14.3.7 was not released).

In 14.3 RU1, the Symantec Endpoint Protection client for Linux was renamed to the Symantec Single Agent for Linux.

If you have a build number but you are not sure how it translates to release version, see:

[About Endpoint Protection release types and versions](#)

Unsupported upgrade paths

You cannot migrate to Symantec Endpoint Protection from all Symantec products. You must uninstall the following products before you install the Symantec Endpoint Protection client.

- Downgrade paths are not supported. For example, if you want to migrate from Symantec Endpoint Protection 14.3 RU8 to 14.3 RU7, you must first uninstall Symantec Endpoint Protection 14.3 RU8.
- 14.3 RU6 and later does not support 32-bit operating systems. Either upgrade your computers to a 64-bit operating system or install 14.3 RU5 for 32-bit operating systems.
- 14.0.x dropped support for Windows XP, Server 2003, and any Windows Embedded operating system that is based on Windows XP. Symantec Endpoint Protection Manager 14.2 RU1 can manage these computers as legacy 12.1.x

clients, although 12.1.x clients are EOL. For these clients, you may want to use a Symantec product that still supports these legacy operating systems, such as Data Center Security (DCS).

- All Symantec Norton products
- Symantec Endpoint Protection for Windows XP Embedded 5.1

Supported paths to the Symantec Endpoint Security cloud console

For the hybrid option:

- *Symantec Endpoint Protection Manager*: Symantec recommends the latest version but a minimum of 14.3 MP1 (14.3.1169.0010).
- *Symantec Endpoint Protection client*: Version 14.3 MP1 (14.3.1169.0010) or later. The client runs on Windows Server 2008 R2 or later and not Windows Server 2008 RTM/SP1/SP2.

See: [Migrating to the SES cloud console](#)

Where to get more information

The following table displays the websites where you can get best practices, troubleshooting information, and other resources to help you use the product.

Table 20: Endpoint Protection website information

Types of information	Website link
Trial versions	Contact your account representative.
Manuals and documentation updates	Related Documents page For other languages, click the language drop-down menu.
Technical Support	Broadcom Technical Support Includes knowledge base articles, product release details, updates and patches, and contact options for support.
Threat information and updates	Symantec Security Center
Training	Education Services Access the training courses, the eLibrary, and more.
Symantec Connect forums	Endpoint Protection - Symantec Enterprise (broadcom.com)

